Attorney Docket No.: 5782.P007 *PATENT*

UNITED STATES PATENT APPLICATION

For

METHOD AND SYSTEM TO PROVIDE SECURE KEY SELECTION USING A SECURE DEVICE IN A WATERCRYPTING ENVIRONMENT

INVENTOR:

ROBERT FRANSDONK

Prepared By:
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026

(408) 947-8200

"Express Mail" mailing label number: EV024657278US
Date of Deposit: February 22, 2002
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Patricia M. Richard
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

February 22, 2002
(Date signed)

METHOD AND SYSTEM TO PROVIDE SECURE KEY SELECTION USING A SECURE DEVICE IN A WATERCRYPTING ENVIRONMENT

RELATED APPLICATIONS

[0001] This patent application is related to U.S. Patent Application Serial No. _____, entitled "Method and System to Provide Secure Key Distribution in a Watercrypting Environment," and filed concurrently herewith.

FIELD OF THE INVENTION

[0002] The present invention relates generally to content distribution in a network environment. More particularly, the present invention relates to the secure distribution of content. Specifically, the present invention relates to a method and system to provide secure key selection using a secure device in a watercrypting environment and to a secure manner to embed a unique fingerprint in the content in order to track unauthorized distribution of the content.

BACKGROUND OF THE INVENTION

[0003] Digital content distribution has increased tremendously with the emergence of Wide Area Networks ("WANs") such as the Internet. For example, users on the Internet can request streaming video content using a video-on-demand type of service. A number of challenges exist, however, for distributing content to users via the Internet. One challenge is preventing illegal copying and distribution of premium content.

[0004] Network operators use a number of content protection systems to prevent illegal copying and distribution of content. One type of content protection system is a

conditional access (CA) system. A CA system imposes restrictions and rules for accessing distributed content. For example, a CA system may control access to content by encrypting the content before distribution and sending decryption keys for users to decrypt the encrypted content. A CA system typically uses entitlement control messages ("ECMs") to deliver the decryption keys to the users. An ECM is a message that includes decryption keys to decrypt encrypted content and rules and requirements to access the decryption keys. In many current CA systems the same encrypted content is broadcasted to multiple users along with its corresponding ECM on the same network. A disadvantage of current CA systems is that the same encrypted content and decryption keys are distributed to all users. Thus, for current CA systems, there is no secure means to create unique content copies for each user.

[0005] Therefore, what is needed is a secure method to deliver ECMs such that authorized users only receive ECMs containing the right decryption keys for decrypting the right piece of content, thereby creating a unique sequence for each user. Further, what is needed is a secure environment and method to select an appropriate session decryption key from the decryption keys delivered within the ECMs in order to decrypt the desired content.

SUMMARY OF THE INVENTION

[0006] A method and system are disclosed to provide secure key selection using a secure device in a watercrypting environment. According to one aspect of the present invention, a license containing a product key of a watercrypted content and a client identifier is transmitted to a secure device for storage. An entitlement control message containing multiple content keys associated with the watercrypted content is further transmitted to the secure device, together with a request to provide a session content key from the multiple content keys, the session content key to be used to decrypt the watercrypted content. Finally, the session content key is received from the secure device in response to the request.

[0007] Other features and advantages of the present invention will be apparent from the accompanying drawings, and from the detailed description, which follows below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention is illustrated by way of example, and not limitation, by the figures of the accompanying drawings in which like references indicate similar elements in which:

[0009] **FIGURE 1** is a block diagram of one embodiment of a watercrypting environment to provide secure key distribution and selection.

[0010] **FIGURE 2** is a block diagram of one embodiment of duplicated and watercrypted content within the watercrypting environment.

[0011] **FIGURE 3** is a flow diagram of one embodiment of a method to provide secure key selection using a secure device in a watercrypting environment.

[0012] **FIGURE 4** is a flow diagram of another embodiment of the method to provide secure key selection using a secure device in a watercrypting environment.

[0013] **FIGURE 5** is a block diagram of an exemplary digital processing or computing system in which the present invention can be implemented.

DETAILED DESCRIPTION

[0014] A method and system are described to provide secure key selection using a secure device in a watercrypting environment. For one embodiment, a license containing a content identifier of a watercrypted content and a client identifier is transmitted to a secure device for storage. An entitlement control message containing multiple content keys associated with the watercrypted content is further transmitted to the secure device, together with a request to provide a session content key from the multiple content keys, the session content key to be used to decrypt the watercrypted content. Finally, the session content key is received from the secure device in response to the request.

[0015] The following embodiments describe secure key distribution and selection in a watercrypting environment such that a client is able to access or decrypt the right piece of watercrypted content. In particular, the following embodiments describe enforcement of a watercrypting process by cryptographically binding unique keys with unique watermark or fingerprint information. In the following description, a "watermark" or "watermark identifier" refers to a fingerprint, identifier, or signature that may be used to indicate copyright protected content. The watermark can also be used to indicate the origin and authenticity of the content or the identity of clients/users/customers of the content.

[0016] In the following description, "watercrypting" or "watercrypt" refer to the process of duplicating content and adding a first watermark identifier to a first piece of duplicated content and a second watermark identifier to a second piece of duplicated content for distribution to a client. Watercrypting also refers to the process of encrypting the duplicated content with unique keys and generating ECMs to distribute securely the unique keys such that unique keys are tied to unique watermark identifiers.

[0017] Furthermore, in the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be evident, however, to one skilled in the art that the present invention may be practiced without these specific details.

[0018] **Figure 1** is a block diagram of one embodiment of a watercrypting environment to provide secure key distribution and selection. Secure key distribution is implemented by a watercrypting process that cryptographically binds unique keys with unique watermark or fingerprint information.

[0019] Referring to **Figure 1**, content server 103 performs a watercrypting process in network environment 100 to create watercrypted content. Content server 103 also distributes watercrypted content to client 106 via content distribution network 102. Content server 103 can also distribute keys to client 106 via secure key distribution network 104. In one embodiment, content server 103 generates entitlement control messages ("ECMs") to deliver the keys to client 106. In the following embodiments, such ECMs are messages that include encrypted keys tied to unique segments of watercrypted content. Client 106 receives the ECMs on the secure key distribution network 104 and selectively selects the unique keys in the ECMs to access watercrypted content from content server 103, as described in further detail below.

[0020] In the embodiment of **Figure 1**, content server 103 is shown to communicate with a single client 106, however, content server 103 may communicate with any number of clients connected to content distribution network 102. In one embodiment, content distribution network 102 is the Internet. The Internet is a worldwide system of interconnected networks that runs the Internet Protocol (IP) to transfer data (e.g., packets). In other embodiments, network 102 can be other types of networks such as, for

example, a token ring network, local area network (LAN), or a wide area network (WAN). Network 102 can also be implemented in a wired or wireless environment. Network 102 can also be implemented using a known Moving Picture Experts Group (MPEG-2) digital video distribution network.

[0021] Secure key distribution network 104 is shown as a separate network restricted to content server 103 and client 106. For example, content server 103 may connect with client 106 via a modem connection. Client 106 may use a secure device 120, such a smart card, to allow for secured communication with content server 103. In other embodiments, secure key distribution network 104 may be a subnetwork within content distribution network 102. Secure key distribution network 104 is used to deliver securely ECMs to client 106.

[0022] Content server 103 embodies a general-purpose computer such as a web server. Content server 103 may also embody a network device such as a network router, switch, bridge, gateway, or other like network device to perform the operations described herein. Content server 103 includes a watercrypt encoder 101 to receive, e.g., compressed audio/video data, and to watercrypt the data into duplicated watercrypted content for distribution to client 106 on content distribution network 102. Watercrypt encoder 101 also generates ECMs to deliver keys (for accessing the watercrypted content) to client 106 on the secure key distribution network 104. Such processes for content server 103 will be described in further detail below.

[0023] In one embodiment, watercrypt encoder 101 is a programmable hardware and/or software module to perform the watercrypting and secure key distribution operations described herein. For example, watercrypt encoder 101 may be a programmable software module executed by a processor within content server 103 to

perform operations such as watercrypting and ECM generation and distribution. Alternatively, watercrypt encoder 101 may be programmable hardware such as a field programmable gate array (FPGA) device that is programmed to perform the same operations.

[0024] Watercrypt encoder 101 may receive compressed audio/video in varying standards such as Moving Picture Experts Group (MPEG), digital video broadcast (DVB), or other like standards. The compressed audio/video may be stored in transport storage 112. Transport storage 112 may include storage devices such as a hard disk, compact disk (CD), digital video disc (DVD), a random access memory (RAM), a dynamic random access memory (DRAM), or other like memory devices contained in or coupled to content server 103.

[0025] Client 106 embodies a general-purpose computer for receiving watercrypted content from content server 103 via content distribution network 102. Client 106 also receives ECMs from content server 103 on secure key distribution network 104. Alternatively, client 106 may be another content server such as content server 103. For example, client 106 may embody a personal computer, workstation, laptop computer, or other like computing devices. Client 106 may also embody an electronic portable devices such as a personal data assistant (PDA), wireless telephone, or other like devices, which can communicate with content distribution network 102 over a wired or wireless medium.

[0026] Client 106 includes a watercrypt decoder 111 to receive watercrypted content and corresponding content keys in ECMs from content server 103. Client 106 also includes a secure device 120, for example a smart card device, to communicate with the watercrypt decoder 111. The secure device 120 further provides selected session content keys to the watercrypt decoder 111 to allow the decoder 111 to access or decrypt

watercrypted content received from content server 103, as described in further detail below. Client 106 further includes applications to view and display the decrypted watercrypted content from content server 103. For example, client 106 may use an application such as, for example, Real Player™ or QuickTime™ to play back the decrypted watercrypted content.

[0027] In one embodiment, watercrypt encoder 101 duplicates a certain subset of compressed audio/video data and watermarks the duplicated content with a first watermark identifier and second watermark identifier. The duplicated content is then encrypted with unique content keys.

[0028] For example, a certain segment of content is duplicated with a first watermark identifier and a second watermark identifier. In one embodiment, a first watermark identifier refers to a "1" and a second watermark identifier refers to a "0". The watermark identifiers, however, may refer to any number of different combinations of "1s" or "0s" or alpha-numeric symbols.

[0029] As illustrated in **Figure 2**, which is a block diagram of one embodiment of duplicated and watercrypted content within the watercrypting environment, each copy is encrypted with a different content segment encryption key K_{m0} and K_{m1}. For example, watercrypt encoder 101 encrypts the duplicated content C_{M0} and C_{M1} with different segment or time-varying content keys K_{m0} and K_{m1}, respectively. The following labels refer to the different segments of content and corresponding keys to encrypt the segments as shown in diagram 200 of **Figure 2**:

[0030] c_m: clear content for period m, before watermarking and encryption;

c_{m0}: content for period m, watermarked with 0;

c_{m1}: content for period m, watermarked with 1;

k_{m0}: key used to encrypt content for period m, watermarked with 0; and

k_{m1}: key used to encrypt content for period m, watermarked with 1.

[0031] The content period "m" may also refer to an identifier to the particular segment of content. The watercrypting process performed by watercrypt encoder 101 can be defined by a watercryption process (Q) including a watermarking (W) process and an encryption (E) process. With respect to watercrypted content of **Figure 2**, watercrypt encoder 101 performs an operation or process defined by **Equation 1**:

[0032] **Equation 1**

$$Q(c_m) = E(k_{m0}, W_0(c_m)) + E(k_{m1}, W_1(c_m))$$

[0033] In **Equation 1**, the encryption process (E) may use any arbitrary or standard encryption algorithm and the watermarking process (W) may also use any arbitrary or standard watermarking algorithm.

[0034] Subsequent to the watercrypting process, the entitlement control messages (ECMs) are generated for client 106 based on a client identifier, for example a watermark ID (WID) for client 106, and based on a segment number for each segment of the duplicated content. Also, watercrypt encoder 101 encrypts the individual content keys using a content identifier to create the ECMs, for example a product key "p." The ECMs are constructed as defined by **Equation 2** below:

[0035] **Equation 2**

$$m + d + E_p(K_{m0} + K_{m1}) + Signature_p(m + d + E_p(K_{m0} + K_{m1}))$$

[0036] In **Equation 2**, "d" represents an arbitrary access criteria data that is signed along with the ECM and "m" represents the period/content segment number or identifier. In one embodiment, m is a cyclic value between 0 and n, e.g., (0, 1, 2, ..., n-1). The value

of n determines the number of unique watermarks or fingerprints that can be generated, which is 2" in case of a binary watermark ('0' or '1'). For example, n=16 provides for a maximum of 65536 unique fingerprints.

[0037] Thus, watercrypt encoder 101 may sign the entire message with the product key "p". This allows another secure device, such as client 106, holding the same product key to verify securely which keys are intended for which content segments/watermark based on the value of m, which is included in the ECM.

[0038] As will be explained in further detail below, content server 103 may therefore be able to provide selectively content keys to client 106 or other clients on the basis of the value of m and the intended watermark identification information "WID". The WID may simply be a number assigned to the secure device 120, e.g., a smart card address for the client 106 or a number assigned to a transaction, e.g., a transaction ID, which in turn may identify a secure device and, thus, the subscriber or client.

[0039] In one embodiment, watercrypt encoder 101 can send duplicated content C_{M0} and C_{M1}, as shown in **Figure 2**, to client 106 via content distribution network 102. Each segment of the duplicated content is encrypted with the unique content keys K_{m0} and K_{m1}. The watercrypt encoder 101 can further distribute the ECMs to client 106 over the secure key distribution network 104.

[0040] In one embodiment, both content server 103 and client 106 include a key selection process such that content server 103 can selectively distribute ECMs with a particular WID and segment number or client 106 can selectively select ECMs with the particular WID and segment number as will be described below.

[0041] In one embodiment, a simple algorithm may be used based on the segment number "m" and the watermark identification information "WID." For example, a key selection process as defined by **Equation 3** may be used:

[0042] **Equation 3**

KeySelector(m) = wid[m%l]

[0043] In **Equation 3**, "l" is the length wid and "%" represents the "mod" operation. In addition, m is a cyclic value between 0 and n and m is a multiple of 1. For example, assuming n=256, wid = '01100110' and I=8:

[0044] KeySelector(0) = 0

KeySelector(1) = 1

KeySelector(2) = 1

...

KeySelector(8) = 0

KeySelector(9) = 1

...

[0045] Referring back to **Figure 2**, using the above key selection process, the duplicated content for segment "0" would require decrypting the corresponding segment of watercrypted content watermarked with "0" using the corresponding encryption key. Thus, using the above key selection process, the keys used by client 106 can be predetermined. Furthermore, content server 103 may also include the same key selection process to distribute selectively those ECMs having those corresponding decryption keys.

[0046] In the example of **Figure 1**, the key selection process yields a key selection of "1011" such that client 106 selects those decryption keys for corresponding content watermarked with "1011". In one embodiment, content server 103 may broadcast ECMs

on secure key distribution network 104. Thus, without using a correct key selection process as described above, a client connected to secure key distribution network 104 will not be able to select the correct ECMs and thus correct decryption keys.

[0047] **Figure 3** is a flow diagram of one embodiment of a method to provide secure key selection using a secure device in a watercrypting environment. As shown in **Figure 3**, at processing block 310, the watercrypt decoder 111 within the client 106 receives the watercrypted content from the watercrypt encoder 101 within the content server 103 via the content distribution network 102.

[0048] At processing block 320, the watercrypt decoder 111 within the client 106 receives a license containing the transaction ID or "WID" and the product key "p" encrypted with a public key of the secure device 120 via the secure key distribution network 104. In one embodiment, the watercrypt encoder 101 encrypts the product key "p" with the public key of the secure device 120 and appends the WID to create the license. Alternatively, the watercrypt encoder 101 may encrypt the product key "p" with a private or secret key of the secure device 120. In yet another alternate embodiment, the license may be created by another entity, for example an agent connected to the secure key distribution network 104 and configured to receive the license information from the content server 103 and to encrypt the product key with the public key of the secure device.

[0049] At processing block 330, the watercrypt decoder 111 transmits the license to the secure device 120. The secure device 120 stores the license and secures access to the product key "p," which was previously encrypted with the public key of the secure device 120.

[0050] At processing block 340, a decision is made by the watercrypt decoder 111 whether to establish a secure channel with the secure device 120. The secure channel allows the secure transmission of communications between the decoder 111 and the secure device 120.

[0051] If the decoder 111 decides to establish the secure channel, at processing block 345, a transport key is encrypted with the public key of the decoder 111. The decoder 111 subsequently transmits the transport key to the secure device 120. At processing block 350, the decoder 111 receives a message containing the unique content keys corresponding to the watercrypted content. In one embodiment, the message is an ECM transmitted via the secure key distribution network 104. At processing block 355, the decoder 111 transmits the message to the secure device 120. At the same time, the watercrypt decoder 111 transmits a request for a session content key to be used to decrypt the watercrypted content, e.g. one of the content keys K_{m0} or K_{m1}. Finally, at processing block 360, the decoder 111 receives the session content key encrypted with the transport key from the secure device 120 and proceeds to decrypt the watercrypted content.

[0052] If the decoder 111 decides not to establish the secure channel, at processing block 365, the decoder 111 receives a message containing the unique content keys corresponding to the watercrypted content. In one embodiment, the message is the ECM transmitted via the secure key distribution network 104, which contains the content keys K_{m0} and K_{m1}. At processing block 370, the decoder 111 transmits the message to the secure device 120. At the same time, the watercrypt decoder 111 transmits the request for the session content key to be used to decrypt the watercrypted content. Finally, at processing block 375, the decoder 111 receives the session content key from the secure device 120 and proceeds to decrypt the watercrypted content.

[0053] **Figure 4** is a flow diagram of another embodiment of the method to provide secure key selection using a secure device in a watercrypting environment. As shown in **Figure 4**, at processing block 410, the secure device 120 receives the license from the watercrypt decoder 111. In one embodiment, the license contains the transaction ID or "WID" and the product key "p" encrypted with the public key of the secure device 120.

[0054] At processing block 420, a decision is made whether a secure channel between the secure device 120 and the decoder 111 needs to be established. In one embodiment, the decoder 111 decides whether to establish the secure channel with the secure device 120.

[0055] If the secure channel is established, at processing block 425, the secure device 120 receives the transport key encrypted with the public key of the decoder 111. At processing block 430, the secure device 120 receives a message containing the unique content keys corresponding to the watercrypted content from the watercrypt decoder 111. In one embodiment, the message is an ECM transmitted via the secure key distribution network 104. At the same time, the secure device 120 receives a request for the session content key to be used to decrypt the watercrypted content, e.g. one of the content keys K_{m0} or K_{m1}. At processing block 435, the secure device 120 selects the session content key using the product key "p" and the WID received in the license. At processing block 440, the secure device encrypts the session content key using the transport key of the secure channel. Finally, at processing block 445, the secure device 120 transmits the session content key encrypted with the transport key to the decoder 111.

[0056] If the secure channel is not established, at processing block 450, the secure device 120 receives the message containing the unique content keys corresponding to the watercrypted content from the watercrypt decoder 111. At the same time, the secure

device 120 receives the request for the session content key to be used to decrypt the watercrypted content, e.g. one of the content keys K_{m0} or K_{m1}. At processing block 455, the secure device 120 selects the session content key using the product key "p" and the WID received in the license. Finally, at processing block 460, the secure device 120 transmits the session content key to the watercrypt decoder 111.

[0057] **Figure 5** is a block diagram of an exemplary digital processing system 500 for a content server or a client. For example, digital processing system 500 can represent content server 103 or client 106 as described in **Figure 1**. Digital processing system 500 may store a set of instructions for causing the system to perform any of the operations as explained above. Digital processing system 500 can also represent a network device, which includes a network router, switch, bridge, or gateway. Digital processing system 500 can also represent a client as a portable electronic device such as, for example, a personal data assistant, a mobile device, a web appliance, or any other type of machine capable of executing a sequence of instructions that specify actions to be taken by that device.

[0058] Referring to **Figure 5**, digital processing system 500 includes a bus 508 coupled to a central processing unit (CPU) 502, main memory 504, static memory 506, network interface 522, video display 510, alpha-numeric input device 512, cursor control device 514, drive unit 516, and signal generation device 520. The devices coupled to bus 508 can use bus 508 to communicate information or data to each other. Furthermore, the devices of digital processing system 500 are exemplary in which one or more devices can be omitted or added. For example, one or more memory devices can be used for digital processing system 500.

[0059] The CPU 502 can process instructions 526 or instructions 526 stored in main memory 504 or a machine-readable medium 524 within drive unit 516 via bus 508. For one embodiment, CPU 502 can process and execute instructions 526 to implement the operations described above. Bus 508 is a communication medium for communicating data or information for digital processing system 500.

[0060] Main memory 504 can be, e.g., a random access memory (RAM) or some other dynamic storage device. Main memory 504 stores instructions 526, which can be used by CPU 502. Main memory 504 may also store temporary variables or other intermediate information during execution of instructions by CPU 502. Static memory 506, can be, e.g., a read only memory (ROM) and/or other static storage devices, for storing information or instructions, which can also be used by CPU 502. Drive unit 516 can be, e.g., a hard or floppy disk drive unit or optical disk drive unit, having a machine-readable medium 524 storing instructions 526. The machine-readable medium 524 can also store other types of information or data.

[0061] Video display 510 can be, e.g., a cathode ray tube (CRT) or liquid crystal display (LCD). Video display device 510 displays information or graphics to a user. Alpha-numeric input device 512 is an input device (e.g., a keyboard) for communicating information and command selections to digital processing system 500. Cursor control device 514 can be, e.g., a mouse, a trackball, or cursor direction keys, for controlling movement of an object on video display 510. Signal generation device 520 can be, e.g., a speaker or a microphone.

[0062] Digital processing system 500 can be connected to a network 102 via a network interface device 522. Network interface 522 can connect to a network such as, for example, a local area network (LAN), wide area network (WAN), token ring network,

Internet, or other like networks. Network interface device 522 can also support varying network protocols such as, for example, hypertext transfer protocol (HTTP), asynchronous transfer mode (ATM), fiber distributed data interface (FDDI), frame relay, or other like protocols.

[0063] It is to be understood that embodiments of this invention may be used as or to support software programs executed upon some form of processing core (such as the CPU of a computer) or otherwise implemented or realized upon or within a machine or computer readable medium. A machine readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine readable medium includes read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); or any other type of media suitable for storing or transmitting information.

[0064] Thus, a method and system to provide secure key selection in a watercrypting environment using a secure device have been described. In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.